



## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets <sup>7</sup> : H04L 9/06	A1	(11) Numéro de publication internationale: WO 00/24155 (43) Date de publication internationale: 27 avril 2000 (27.04.00)
--	----	---

(21) Numéro de la demande internationale: PCT/FR99/02172

(22) Date de dépôt international: 13 septembre 1999 (13.09.99)

(30) Données relatives à la priorité:  
98/12989 16 octobre 1998 (16.10.98) FR

(71) Déposant (pour tous les Etats désignés sauf US): GEM-PLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (US seulement): CLAVIER, Christophe [FR/FR]; 5 rue de la République, F-13420 Gémenos (FR).  
BENOIT, Olivier [FR/FR]; La Treille d'Azur, Bâtiment D. avenue 19 Mars 1962, F-13400 Aubagne (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos Cedex (FR).

(81) Etats désignés: AU, CA, CN, IN, JP, MX, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

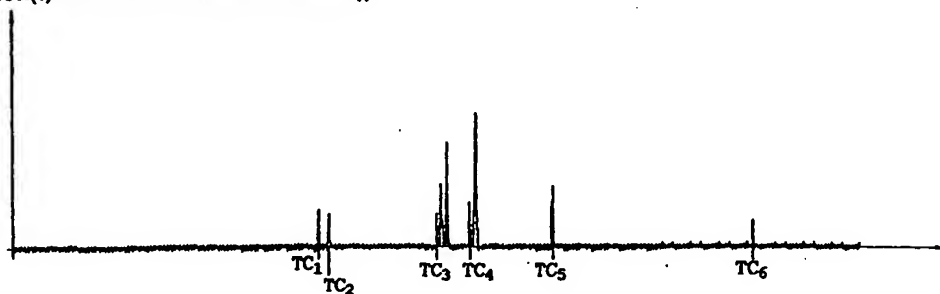
Publiée

Avec rapport de recherche internationale.

(54) Title: COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM

(54) Titre: PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE SECRETE

DPA(t) DIFFERENTIAL POWER ANALYSIS SIGNAL (n)



## (57) Abstract

The invention concerns a countermeasure method in an electronic component using a secret key K cryptographic algorithm, wherein the algorithm implementation comprises the use of first means TC<sub>0</sub> for supplying output data from input data, the output information and/or derived data being manipulated by critical instructions. Said countermeasure method provides for the use of other means TC<sub>1</sub> and/or TC<sub>2</sub>, such that the output information and the derived data are unpredictable.

## (57) Abrégé

Dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète K, la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers moyens TC<sub>0</sub> pour fournir une donnée de sortie S à partir d'une donnée d'entrée E, la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques, un procédé de contre-mesure prévoit l'utilisation d'autres moyens TC<sub>1</sub> et/ou TC<sub>2</sub>, en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

# **UNIQUEMENT A TITRE D'INFORMATION**

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brazil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroon	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

**PROCÉDÉ DE CONTRE-MESURE DANS UN COMPOSANT  
ÉLECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE  
CRYPTOGRAPHIE A CLÉ SECRÈTE**

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme de cryptographie à clé secrète. Ils sont utilisés dans des applications où l'accès à des services ou à des données est sévèrement contrôlé. Ils ont une architecture formée autour d'un microprocesseur et de mémoires, dont une mémoire programme qui contient la clé secrète.

Ces composants sont notamment utilisés dans les cartes à puce, pour certaines applications de celles-ci. Ce sont par exemple des applications d'accès à certaines banques de données, des applications bancaires, des applications de télépéage, par exemple pour la télévision, la distribution d'essence ou encore le passage de péages d'autoroutes.

Ces composants ou ces cartes mettent donc en oeuvre un algorithme de cryptographie à clé secrète, dont le plus connu est l'algorithme DES (pour *Data Encryption Standard* dans la littérature anglo-saxonne). D'autres algorithmes à clé secrète existent, comme l'algorithme RC5 ou encore l'algorithme COMP128. Cette liste n'est bien sûr pas exhaustive.

De manière générale et succincte, ces algorithmes ont pour fonction de calculer un message chiffré à partir d'un message appliqué en entrée (à la carte) par un système hôte (serveur, distributeur bancaire...) et de la clé secrète contenue dans la carte, et de fournir en retour au système hôte ce message chiffré, ce qui permet par exemple au système hôte d'authentifier le composant ou la carte, d'échanger des données...

Or il est apparu que ces composants ou ces cartes sont vulnérables à des attaques consistant en une analyse différentielle de consommation en courant et qui permettent à des tiers mal intentionnés de trouver la clé secrète. Ces attaques sont appelées attaques DPA, acronyme anglo-saxon pour *Differential Power Analysis*.

Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

Notamment, une instruction du microprocesseur manipulant un bit de donnée génère deux profils de courant différents selon que ce bit vaut "1" ou "0". Typiquement, si l'instruction manipule un "0", on a à cet instant d'exécution une première amplitude du courant consommé et si l'instruction manipule un "1", on a une deuxième amplitude du courant consommé, différente de la première.

Les caractéristiques des algorithmes de cryptographie sont connues : calculs effectués, paramètres utilisés. La seule inconnue est la clé secrète contenue en mémoire programme. Celle-ci ne peut être déduite de la seule connaissance du message appliqué en entrée et du message chiffré fourni en retour.

Cependant, dans un algorithme de cryptographie, certaines données calculées dépendent seulement du message appliqué en clair en entrée de la carte et de la clé secrète contenue dans la carte. D'autres données calculées dans l'algorithme peuvent aussi être recalculées seulement à partir du message chiffré (généralement fourni en clair en sortie de la carte vers le système hôte) et de la clé secrète contenue dans la carte. Plus précisément, chaque bit de ces données particulières peut être déterminé à partir du

message d'entrée ou de sortie, et d'un nombre limité de bits particuliers de la clé.

Ainsi, à chaque bit d'une donnée particulière, correspond une sous-clé formée par un groupe  
5 particulier de bits de la clé.

Les bits de ces données particulières qui peuvent être prédites sont appelés dans la suite, bits cibles.

L'idée de base de l'attaque DPA est ainsi  
10 d'utiliser la différence du profil de consommation en courant d'une instruction selon qu'elle manipule un "1" ou un "0" et la possibilité de calculer un bit cible par les instructions de l'algorithme à partir d'un message connu d'entrée ou de sortie et d'une hypothèse sur la sous-clé correspondante.

15 Le principe de l'attaque DPA est donc de tester une hypothèse de sous-clé donnée, en appliquant sur un grand nombre de courbes de mesure en courant, chacune relative à un message d'entrée connu de l'attaquant, une fonction booléenne de sélection, fonction de  
20 l'hypothèse de sous-clé, et définie pour chaque courbe par la valeur prédite pour un bit cible.

En faisant une hypothèse sur la sous-clé concernée, on est en effet capable de prédire la valeur "0" ou "1" que va prendre ce bit cible pour un message d'entrée ou  
25 de sortie donné.

On peut alors appliquer comme fonction booléenne de sélection, la valeur prédite "0" ou "1" par le bit cible pour l'hypothèse de sous-clé considérée, pour trier ces courbes en deux paquets : un premier paquet  
30 regroupe les courbes qui ont vu la manipulation du bit cible à "0" et un deuxième paquet regroupe les courbes qui ont vu la manipulation du bit cible à "1" selon l'hypothèse de sous-clé. En faisant la moyenne de consommation en courant dans chaque paquet, on obtient  
35 une courbe de consommation moyenne  $M_0(t)$  pour le

premier paquet et une courbe de consommation moyenne  $M_1(t)$  pour le deuxième paquet.

Si l'hypothèse de sous-clé est juste, le premier paquet regroupe réellement toutes les courbes parmi les  
 5 N courbes qui ont vu la manipulation du bit cible à "0" et le deuxième paquet regroupe réellement toutes les courbes parmi les N courbes qui ont vu la manipulation du bit cible à "1". La courbe moyenne de consommation  $M_0(t)$  du premier paquet aura alors une consommation  
 10 moyenne partout sauf aux moments de l'exécution des instructions critiques, avec un profil de consommation en courant caractéristique de la manipulation du bit cible à "0" ( $\text{profil}_0$ ). En d'autres termes, pour toutes ces courbes tous les bits manipulés ont eu autant de  
 15 chances de valoir "0" que de valoir "1", sauf le bit cible qui a toujours eu la valeur "0". Ce qui peut s'écrire :

$$M_0(t) = [(\text{profil}_0 + \text{profil}_1)/2]_{t \neq t_{ci}} + [\text{profil}_0]_{t_{ci}} \text{ soit}$$

$$M_0(t) = [V_{m_t}]_{t \neq t_{ci}} + [\text{profil}_0]_{t_{ci}}$$

20 où  $t_{ci}$  représente les instants critiques, auxquels une instruction critique a été exécutée.

De même, la courbe moyenne de consommation  $M_1(t)$  du deuxième paquet correspond à une consommation moyenne partout sauf aux moments de l'exécution des  
 25 instructions critiques, avec un profil de consommation en courant caractéristique de la manipulation du bit cible à "1" ( $\text{profil}_1$ ). On peut écrire :

$$M_1(t) = [(\text{profil}_0 + \text{profil}_1)/2]_{t \neq t_{ci}} + [\text{profil}_1]_{t_{ci}} \text{ soit}$$

$$M_1(t) = [V_{m_t}]_{t \neq t_{ci}} + [\text{profil}_1]_{t_{ci}}$$

30 On a vu que les deux profils  $\text{profil}_0$  et  $\text{profil}_1$  ne sont pas égaux. La différence des courbes  $M_0(t)$  et  $M_1(t)$  donne alors un signal  $DPA(t)$  dont l'amplitude est égale à  $\text{profil}_0 - \text{profil}_1$  aux instants critiques  $t_{ci}$  d'exécution des instructions critiques manipulant ce  
 35 bit, c'est à dire, dans l'exemple représenté sur la figure 1, aux endroits  $tc_0$  à  $tc_6$ , et dont l'amplitude

est à peu près égale à zéro en dehors des instants critiques.

Si l'hypothèse de sous-clé est fausse, le tri ne correspond pas à la réalité. Statistiquement, il y a alors dans chaque paquet, autant de courbes ayant vu réellement la manipulation du bit cible à "0" que de courbes ayant vu la manipulation du bit cible à "1". La courbe moyenne résultante  $M0(t)$  se situe alors autour d'une valeur moyenne donnée par  $(profil_0 + profil_1)/2 = V_m$ , car pour chacune des courbes, tous les bits manipulés, y compris le bit cible ont autant de chances de valoir "0" que de valoir "1".

Le même raisonnement sur le deuxième paquet conduit à une courbe moyenne de consommation en courant  $M1(t)$  dont l'amplitude se situe autour d'une valeur moyenne donnée par  $(profil_0 + profil_1)/2 = V_m$ .

Le signal  $DPA(t)$  fourni par la différence  $M0(t) - M1(t)$  est dans ce cas sensiblement égal à zéro. Le signal  $DPA(t)$  dans le cas d'une hypothèse de sous-clé fausse est représenté sur la figure 2.

Ainsi l'attaque DPA exploite la différence du profil de consommation en courant pendant l'exécution d'une instruction suivant la valeur du bit manipulé, pour effectuer un tri de courbes de consommation en courant selon une fonction de sélection booléenne pour une hypothèse de sous-clé donnée. En effectuant une analyse différentielle de la consommation moyenne en courant entre les deux paquets de courbes obtenus, on obtient un signal d'information  $DPA(t)$ .

Le déroulement d'une attaque DPA consiste alors globalement:

a- à tirer N messages aléatoires (par exemple N égal 1000);

b- à faire exécuter l'algorithme par la carte pour chacun des N messages aléatoires, en relevant la courbe

de consommation en courant à chaque fois (mesurée sur la borne d'alimentation du composant);

c- à faire une hypothèse sur une sous-clé;

5 d- à prédire, pour chacun des messages aléatoires, la valeur prise par un des bits cibles dont la valeur ne dépend que des bits du message (d'entrée ou de sortie) et de la sous-clé prise en hypothèse, pour obtenir la fonction de sélection booléenne;

10 e- à trier les courbes selon cette fonction de sélection booléenne (c'est à dire selon la valeur "0" ou "1" prédite pour ce bit cible pour chaque courbe sous l'hypothèse de sous-clé);

f- à calculer dans chaque paquet la courbe résultante de consommation moyenne en courant;

15 g- à effectuer la différence de ces courbes moyennes, pour obtenir le signal DPA(t).

Si l'hypothèse sur la sous-clé est juste, la fonction de sélection booléenne est juste et les courbes du premier paquet correspondent réellement aux courbes pour lesquelles le message appliqué en entrée ou en sortie a donné un bit cible à "0" dans la carte et les courbes du deuxième paquet correspondent réellement aux courbes pour lesquelles le message appliqué en entrée ou en sortie a donné un bit cible à "1" dans la carte.

25 On est dans le cas de la figure 1 : le signal DPA(t) n'est donc pas nul aux instants  $t_{c0}$  à  $t_{c6}$  correspondant à l'exécution des instructions critiques (celles qui manipulent le bit cible).

30 On notera que l'attaquant n'a pas besoin de connaître avec précision les instants critiques. Il suffit qu'il y ait au moins un instant critique dans la période d'acquisition.

35 Si l'hypothèse de sous-clé n'est pas juste, le tri ne correspond pas à la réalité et on a alors dans chaque paquet autant de courbes correspondant en



réalité à un bit cible à "0" que de courbes correspondant à un bit cible à "1". Le signal  $DPA(t)$  est sensiblement nul partout (cas représenté à la figure 2). Il faut retourner à l'étape c- et faire une  
5 nouvelle hypothèse sur la sous-clé.

Si l'hypothèse s'avère juste, on peut passer à l'évaluation d'autres sous-clés, jusqu'à avoir reconstitué la clé au maximum. Par exemple, avec un algorithme DES, on utilise une clé de 64 bits, dont  
10 seulement 56 bits utiles. Avec une attaque DPA, on est capable de reconstituer au moins 48 bits des 56 bits utiles.

La présente invention a pour but de mettre en oeuvre dans un composant électronique, un procédé de contre-mesure qui entraîne un signal  $DPA(t)$  nul, même  
15 dans le cas où l'hypothèse de sous-clé est juste.

De cette façon, rien ne permet de distinguer le cas de l'hypothèse de sous-clé juste des cas d'hypothèses de sous-clé fausses. Par cette contre-mesure, le  
20 composant électronique est paré contre les attaques DPA.

Selon l'invention, le procédé de contre-mesure permet de rendre imprédictibles les bits cibles, c'est à dire les données manipulées par des instructions  
25 critiques.

En effet, du fait de la contre-mesure, pour chaque message appliqué en entrée, un bit cible manipulé par une instruction critique prend la valeur 0 ou 1 avec une égale probabilité. Dans chaque paquet de courbes  
30 que fera l'attaquant sous une hypothèse de sous-clé donnée, au moyen de la fonction de sélection booléenne qu'il aura calculée, on aura autant de courbes ayant réellement manipulé un bit cible "0" que de courbes ayant réellement manipulé un bit cible à "1". Le signal  
35  $DPA(t)$  sera toujours nul, que l'hypothèse de sous-clé soit juste ou non.

Telle que caractérisée, l'invention concerne donc un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète, la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers moyens pour fournir une donnée de sortie à partir d'une donnée d'entrée, la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques. Selon l'invention, le procédé de contre-mesure prévoit l'utilisation d'autres moyens, en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

Selon l'invention, l'utilisation des différents moyens est gérée selon une loi statistique de probabilité un demi.

D'autres caractéristiques et avantages de l'invention sont détaillés dans la description suivante faite à titre indicatif et nullement limitatif et en référence aux dessins annexés, dans lesquels :

- les figures 1 et 2 déjà décrites représentent le signal  $DPA(t)$  que l'on peut obtenir en fonction d'une hypothèse sur une sous-clé de la clé secrète  $K$ , selon une attaque DPA;
- les figures 3 et 4 sont des organigrammes d'exécution des premiers tours et derniers tours de l'algorithme DES;
- la figure 5 est un schéma-bloc de l'opération SBOX utilisée dans l'algorithme DES;
- la figure 6 montre un exemple de table de constante élémentaire à une entrée et une sortie utilisée dans l'opération SBOX;
- les figures 7 et 8 montrent un exemple d'organigramme d'exécution des premiers et derniers tours de l'algorithme DES, selon un mode de réalisation du procédé de contre-mesure selon l'invention;

- les figures 9 et 10 montrent respectivement une deuxième et une troisième tables de constantes élémentaires selon l'invention;

5 - la figure 11 représente un organigramme général d'exécution du DES selon un mode de réalisation du procédé de contre-mesure selon l'invention; et

10 - la figure 12 représente un schéma-bloc simplifié d'une carte à puce comportant un composant électronique dans lequel le procédé de contre-mesure selon l'invention est mis en oeuvre.

La présente invention va être expliquée dans un exemple d'application à l'algorithme cryptographique DES. L'invention n'est pas limitée à ce seul exemple.  
15 Elle s'applique aux algorithmes cryptographiques à clé secrète en général.

L'algorithme cryptographique DES (dans la suite on parlera plus simplement du DES ou de l'algorithme DES) comporte 16 tours de calcul, notés T1 à T16, comme  
20 représenté sur les figures 3 et 4.

Le DES débute par une permutation initiale IP sur le message d'entrée M (figure 3). Le message d'entrée M est un mot f de 64 bits. Après permutation, on obtient un mot e de 64 bits, que l'on coupe en deux pour former  
25 les paramètres d'entrée L0 et R0 du premier tour (T1). L0 est un mot d de 32 bits contenant les 32 bits de poids forts du mot e. R0 est un mot h de 32 bits contenant les 32 bits de poids faibles du mot e.

La clé secrète K, qui est un mot q de 64 bits subit  
30 elle-même une permutation et une compression pour fournir un mot r de 56 bits.

Le premier tour comprend une opération EXP PERM sur le paramètre R0, consistant en une expansion et une permutation, pour fournir en sortie un mot l de 48  
35 bits.

Ce mot l est combiné à un paramètre K1, dans une opération de type OU EXCLUSIF notée XOR, pour fournir un mot b de 48 bits. Le paramètre K1 qui est un mot m de 48 bits est obtenu du mot r par un décalage d'une position (opération notée SHIFT sur les figures 3 et 4) suivi d'une permutation et d'une compression (opération notée COMP PERM).

Le mot b est appliqué à une opération notée SBOX, en sortie de laquelle on obtient un mot a de 32 bits. Cette opération particulière sera expliquée plus en détail en relation avec les figures 5 et 6.

Le mot a subit une permutation P PERM, donnant en sortie le mot c de 32 bits.

Ce mot c est combiné au paramètre d'entrée L0 du premier tour T1, dans une opération logique de type OU EXCLUSIF, notée XOR, qui fournit en sortie le mot g de 32 bits.

Le mot h (=R0) du premier tour fournit le paramètre d'entrée L1 du tour suivant (T2) et le mot g du premier tour fournit le paramètre d'entrée R1 du tour suivant. Le mot p du premier tour fournit l'entrée r du tour suivant.

Les autres tours T2 à T16 se déroulent de façon similaire, excepté en ce qui concerne l'opération de décalage SHIFT qui se fait sur une ou deux positions selon les tours considérés.

Chaque tour Ti reçoit ainsi en entrée les paramètres Li-1, Ri-1 et r et fournit en sortie les paramètres Li, Ri et r pour le tour suivant Ti+1.

En fin d'algorithme DES (figure 4), le message chiffré est calculé à partir des paramètres L16 et R16 fournis par le dernier tour T16.

Ce calcul du message chiffré C comprend en pratique les opérations suivantes :

- formation d'un mot e' de 64 bits en inversant la position des mots L16 et R16, puis en les concaténant;

- application de la permutation  $IP^{-1}$  inverse de celle de début de DES, pour obtenir le mot  $f'$  de 64 bits formant le message chiffré C.

5 L'opération SBOX est détaillée sur les figures 5 et 6. Elle comprend une table de constantes  $TC_0$  pour fournir une donnée de sortie a en fonction d'une donnée d'entrée b.

10 En pratique, cette table de constantes  $TC_0$  se présente sous la forme de huit tables de constantes élémentaires  $TC_{0,1}$  à  $TC_{0,8}$ , chacune recevant en entrée seulement 6 bits du mot b, pour fournir en sortie seulement 4 bits du mot a.

15 Ainsi, la table de constante élémentaire  $TC_{0,1}$  représentée sur la figure 6 reçoit comme donnée d'entrée, les bits  $b_1$  à  $b_6$  du mot b et fournit comme donnée de sortie les bits  $a_1$  à  $a_4$  du mot a.

En pratique ces huit tables de constantes élémentaires sont mémorisées en mémoire programme du composant électronique.

20 Dans l'opération SBOX du premier tour  $T_1$ , un bit particulier de la donnée a de sortie de la table de constante  $TC_0$  dépend de seulement 6 bits de la donnée b appliquée en entrée, c'est à dire de seulement 6 bits de la clé secrète K et du message d'entrée (M).

25 Dans l'opération SBOX du dernier tour  $T_{16}$ , un bit particulier de la donnée a de sortie de la table de constante  $TC_0$  peut être recalculé à partir de seulement 6 bits de la clé secrète K et du message chiffré (C).

30 Or si on reprend le principe de l'attaque DPA, si on choisit comme bit cible un bit de la donnée de sortie a, il suffit de faire une hypothèse sur 6 bits de la clé K, pour prédire la valeur d'un bit cible pour un message d'entrée (M) ou de sortie (C) donné. En d'autres termes, pour le DES, il suffit de faire une  
35 hypothèse sur une sous-clé de 6 bits.

Dans une attaque DPA sur un tel algorithme pour un bit cible donné, on a donc à discriminer une hypothèse de sous-clé juste parmi 64 possibles.

5       Ainsi, en prenant seulement huit bits du mot a comme bits cibles, (un bit de sortie par table de constantes élémentaire  $TC_{01}$  à  $TC_{08}$ ), on peut découvrir jusqu'à  $6 \times 8 = 48$  bits de la clé secrète, en faisant des attaques DPA sur chacun de ces bits cibles.

10       Dans le DES, on trouve donc des instructions critiques au sens des attaques DPA au début de l'algorithme et à la fin.

15       Au début de l'algorithme DES, les données qui peuvent être prédites à partir d'un message d'entrée M et d'une hypothèse de sous-clé, sont les données a et g calculées dans le premier tour (T1).

20       La donnée a du premier tour T1 (figure 3) est la donnée de sortie de l'opération SBOX du tour considéré. La donnée g est calculée à partir de la donnée a, par permutation (P PERM) et opération OU EXCLUSIF avec le paramètre d'entrée L0.

25       En fait, la donnée c du premier tour, est une donnée dérivée de la donnée a du premier tour. La donnée dérivée c correspond à une simple permutation de bits de la donnée a.

30       La donnée l du deuxième tour est une donnée dérivée de la donnée g du premier tour, car elle correspond à une permutation des bits du mot g, certains bits du mot g étant en outre dupliqués.

35       Connaissant a et g, on peut aussi connaître ces données dérivées.

      Les instructions critiques du début de l'algorithme sont les instructions critiques qui manipulent soit la donnée que l'on peut prédire, comme la donnée a du premier tour, soit une donnée dérivée.

      Les instructions critiques manipulant la donnée a du premier tour T1 ou la donnée dérivée c sont ainsi

les instructions de fin de l'opération SBOX, de l'opération P PERM et de début de l'opération XOR du premier tour T1.

5 Les instructions critiques manipulant la donnée g ou des données dérivées sont toutes les instructions de fin d'opération XOR de fin du premier tour T1 jusqu'aux instructions de début d'opération SBOX du deuxième tour T2, et les instructions de début d'opération XOR de fin du troisième tour T3 (  $L2 = h(T2) = g(T1)$  ).

10 En fin d'algorithme DES, les données qui peuvent être prédites à partir d'un message chiffré C et d'une hypothèse de sous-clé, sont la donnée a du seizième tour T16 et la donnée L15 égale au mot h du quatorzième tour T14.

15 Les instructions critiques manipulant la donnée a du seizième tour ou des données dérivées sont les instructions du seizième tour de fin d'opération SBOX, de l'opération de permutation P PERM et de début d'opération XOR.

20 Pour la donnée L15, les instructions critiques manipulant cette donnée ou des données dérivées sont toutes les instructions, depuis les instructions de fin d'opération XOR du quatorzième tour T14, jusqu'aux instructions de début d'opération SBOX du quinzième tour T15, et les instructions de début d'opération XOR de fin du seizième tour T16.

25 Le procédé de contre-mesure selon l'invention appliqué à cet algorithme DES consiste à avoir, pour chaque instruction critique, autant de chances que l'instruction critique manipule une donnée que son complément. Ainsi, quel que soit le bit cible sur lequel l'attaque DPA peut être faite, on a autant de chances que les instructions critiques qui manipulent ce bit, manipulent un "1" ou un "0".

35 En pratique, ceci doit être vrai pour chacun des bits cibles potentiels : en d'autres termes,

l'attaquant ayant le choix entre plusieurs attaques possibles, c'est à dire entre plusieurs fonctions de sélection booléenne possibles pour effectuer son tri de courbes, pour une hypothèse de sous-clé donnée, la mise en oeuvre du procédé de contre-mesure selon l'invention doit s'attacher à ce que les données manipulées par chacune des instructions critiques, prennent aléatoirement, une fois sur deux, une valeur ou son complément. En ce qui concerne l'application du procédé de contre-mesure selon l'invention à l'algorithme DES, il faut donc appliquer la contre-mesure aux instructions critiques de début de DES et aux instructions critiques de fin de DES, pour être totalement protégé.

Dans le DES, toutes les données manipulées par des instructions critiques sont une donnée de sortie ou des données dérivées d'une donnée de sortie d'une opération SBOX.

En effet, en début de DES, les données qui peuvent être prédites sont les données a et g du premier tour T1. La donnée a est la donnée de sortie de l'opération SBOX du premier tour. La donnée g est calculée à partir de la donnée a, puisque  $g = P \text{ PERM}(a) \text{ XOR } L0$ . g est donc une donnée dérivée de la donnée de sortie a de l'opération SBOX du premier tour. Ainsi, toutes les données manipulées par les instructions critiques de début de DES découlent directement ou indirectement de la donnée de sortie a de l'opération SBOX du premier tour.

En ce qui concerne la fin de DES, les données qui peuvent être prédites sont la donnée a du seizième tour T16 et la donnée g du quatorzième tour T14, g étant égale à L15.

La donnée a est la donnée de sortie de l'opération SBOX du seizième tour T16.



Quant à la donnée L15, elle se calcule, dans l'exécution normale de l'algorithme DES, à partir de la donnée de sortie a de l'opération SBOX du quatorzième tour T14 :  $L15 = P \text{ PERM}(a) \text{ XOR } L14$ .

5 Si on rend imprédictibles les données de sortie a de ces opérations SBOX particulières, on rend aussi imprédictibles toutes les données dérivées : on rend donc imprédictibles toutes les données manipulées par les instructions critiques de l'algorithme DES.

10 L'opération SBOX correspond donc à des premiers moyens, qui consistent en une table de constantes  $TC_0$ , et qui sont utilisés dans chaque tour pour fournir une donnée de sortie E à partir d'une donnée d'entrée S.

15 Un mode de réalisation du procédé de contre-mesure appliqué à l'algorithme DES peut consister à utiliser au moins une autre table de constantes comme autres moyens pour rendre imprédictible la donnée de sortie a, en sorte que cette donnée de sortie et/ou des données dérivées manipulées par les instructions critiques  
20 soient toutes imprédictibles.

Dans l'exécution de l'algorithme, l'utilisation des différents moyens, c'est à dire, dans l'exemple, des différentes tables de constantes est gérée selon une loi statistique de probabilité un demi.

25 L'autre table de constantes ou les autres tables de constantes sont telles qu'à l'une et/ou l'autre des données d'entrée d et de sortie de la première table de constantes  $TC_0$ , elles font correspondre la donnée complémentée.

30 Les figures 7 et 8 représentent ainsi un mode d'application du procédé de contre-mesure de l'invention appliqué à l'algorithme DES.

La figure 7 représente le début de l'algorithme. Les opérations et données non modifiées par le procédé  
35 de contre-mesure selon l'invention portent les mêmes références que dans la figure 3 déjà décrite.

En début d'algorithme DES, on prévoit une deuxième table de constante  $TC_1$  dans l'opération SBOX du premier tour T1. Toutes les données affectées par cette deuxième table de constantes  $TC_1$  sont affectées d'un  
5 signe ' ou d'un signe - sur ces figures. On voit que les instructions critiques de début de DES manipulent toutes des données affectées par le procédé de contre-mesure.

On remarquera que la première table de constantes  
10 étant en fait formée de huit premières tables de constantes, la deuxième table de constantes est également formée de huit deuxièmes tables de constantes.

Dans l'exemple de réalisation représenté, la  
15 première table de constantes  $TC_0$  et la deuxième table de constantes  $TC_1$  sont telles que pour une même donnée d'entrée E, la deuxième fournit en sortie le complément /S de la donnée de sortie S fournie par la première.

La figure 9 montre une telle deuxième table  
20 élémentaire  $TC_{11}$  fournissant une sortie complémentée par rapport à la première table élémentaire  $TC_{01}$  montrée sur la figure 6.

Avec une telle deuxième table de constantes  $TC_1$ , on obtient, en sortie de l'opération SBOX du premier tour  
25 T1, le complément /a de la donnée a obtenue avec la première table de constante  $TC_0$ . De même, on obtient dans le premier tour T1 la donnée complémentée /g et dans le deuxième tour T2, les données complémentées /h, /L2, /l et /b.

En utilisant la première table ou la deuxième table  
30 pour fournir la donnée de sortie selon une loi statistique de probabilité un demi, tous les bits de cible potentiels de début de DES manipulés par les instructions critiques ont autant de chances de prendre  
35 la valeur "1" que de prendre la valeur "0".

En fin d'algorithme DES, le mode de réalisation du procédé de contre-mesure selon l'invention nécessite l'utilisation de plusieurs tables de constantes différentes de la première, car il faut considérer à la fois la donnée de sortie a calculée au quatorzième tour T14, et la donnée de sortie a calculée au seizième tour T16 pour rendre imprédictibles toutes les données manipulées par les instructions critiques de cette fin de DES.

10 Un exemple de réalisation du procédé de contre-mesure appliqué à cette fin d'algorithme DES est représenté sur la figure 8.

Il prévoit l'utilisation de deux tables de constantes  $TC_1$  et  $TC_2$ .

15 Dans l'opération SBOX du quatorzième tour T14, on utilise la deuxième table de constantes  $TC_1$  déjà utilisée pour le début du DES.

Et on utilise une troisième table de constantes  $TC_2$ , dans les opérations SBOX des quinzième et seizième tours.

20 Cette troisième table de constantes  $TC_2$  est telle qu'elle fournit le complément /S de la donnée de sortie S au complément /E de la donnée d'entrée E de la première table de constantes  $TC_0$ . Un exemple d'une troisième table de constantes élémentaire  $TC_{21}$  correspondante, à partir de la première table de constantes élémentaire  $TC_0$  est montré sur la figure 10.

25 En utilisant de telles tables de constantes, il apparaît sur la figure 8 que toutes les instructions critiques manipulent des données complémentées.

30 L'invention ne se limite pas à ces seuls exemples de tables de constantes  $TC_1$  et  $TC_2$ . D'autres possibilités existent. Par exemple, pour le procédé de contre-mesure appliqué à la fin de DES, il est aussi possible de combiner l'utilisation de la table de constantes  $TC_1$  avec une autre table de constantes

définie par rapport à la première table de constantes  $TC_0$  comme fournissant la donnée de sortie  $S$  au complément /E. de la donnée d'entrée.

5 D'une manière générale, la fin de DES nécessite l'utilisation de différentes tables de constantes, en fonction des tours considérés, pour que toutes les données manipulées par les instructions critiques de cette fin de DES soient imprédictibles.

10 Le mode de réalisation décrit en relation avec les figures 7 et 8 a cependant un inconvénient : le procédé de contre-mesure appliqué en entrée de DES produit des résultats intermédiaires calculés  $L3'$  et  $R3'$  qui ne sont pas justes. Tous les résultats intermédiaires suivants ne sont donc pas justes non plus.

15 De même, en fin de DES, le procédé de contre-mesure appliqué en entrée de DES produit des résultats intermédiaires calculés  $L16'$  et  $R16'$  qui ne sont pas justes.

Dans tous les cas, le message chiffré est faux.

20 Dans ce mode de réalisation de l'invention, il faut donc prévoir de pouvoir reprendre à chaque fois la suite de l'algorithme avec les bons résultats intermédiaires, une fois les instructions critiques passées.

25 En pratique, comme on a vu que les instructions critiques de début de DES se trouvent dans les trois premiers tours, on va dédoubler ces trois premiers tours. En d'autres termes, on prévoit d'exécuter deux séquences comprenant chacune les trois premiers tours  
30  $T1$ ,  $T2$ ,  $T3$  au moins. Une première séquence SEQA utilise la première table de constantes  $TC_0$  dans chaque tour. L'autre séquence SEQB utilise la deuxième table de constantes  $TC_1$  au moins dans le premier tour  $T1$ . Dans l'exemple représenté, on utilise la première table de  
35 constantes dans les deux tours suivants  $T2$  et  $T3$ .

On a vu que dans le procédé de contre-mesure selon l'invention, l'utilisation des différents moyens, c'est à dire, dans l'exemple, l'utilisation des différentes tables de constantes, est gérée selon une loi statistique de probabilité un demi. Cette loi statistique de probabilité un demi est alors plus particulièrement appliquée à l'ordre d'utilisation de ces différents moyens, c'est à dire, dans l'exemple, à l'ordre d'exécution des deux séquences SEQA et SEQB.

De même, pour avoir les bons paramètres L16 et R16 en fin de DES pour élaborer le message chiffré C, on dédouble également les trois tours T14, T15 et T16 (figure 7) qui contiennent les instructions critiques de fin de DES. On va donc exécuter deux séquences qui comprennent au moins les trois derniers tours T14, T15, T16. Une première séquence SEQA' utilise dans chaque tour la première table de constantes  $TC_0$ . L'autre séquence SEQB' utilise les autres tables de constantes  $TC_1$  et  $TC_2$ . Comme précédemment, la loi statistique de probabilité un demi est alors appliquée à l'ordre d'exécution de ces deux séquences SEQA' et SEQB'.

Les instructions critiques sont alors exécutées deux fois, une dans chaque séquence. Mais au moment de l'exécution de n'importe laquelle des instructions critiques de l'une ou l'autre des séquences, la probabilité de manipuler une donnée sera égale à la probabilité de manipuler son complément.

Le programme de calcul du DES mis en oeuvre dans le composant électronique doit donc être modifié pour inclure le procédé de contre-mesure selon l'invention. Un exemple d'organigramme d'exécution conforme à l'invention et mettant en oeuvre le procédé de contre-mesure en début et en fin de DES selon le mode de réalisation décrit en relation avec les figures 7 et 8 est représenté sur la figure 11. Dans cet exemple, les séquences SEQA et SEQB comprennent les trois premiers

tours et les séquences SEQA' et SEQB' comprennent les trois derniers tours.

Le programme de calcul consiste alors principalement, au début du calcul, à sauvegarder les paramètres d'entrée notés DATAIN et KEY, qui  
5 correspondent en pratique aux paramètres L0, R0 et r, dans une zone mémoire temporaire notée CONTEXT0.

Selon ce programme de calcul, on positionne ensuite un premier compteur de boucle FR à 0, et on tire  
10 aléatoirement une valeur RND1 égale à 0 ou à 1.

Si RND1 vaut 1, dans l'exemple, on effectue d'abord la séquence SEQB de T1, T2, T3, dans laquelle on utilise la deuxième table de constantes TC<sub>1</sub> au tour T1 et la première table TC<sub>0</sub> pour les tours T2 et T3. On  
15 sauvegarde les paramètres de sortie L3', R3' (qui ont des valeurs fausses) dans une zone mémoire temporaire notée CONTEXT2.

Si FR n'est pas égal à 1, on le met à 1, on restaure les paramètres d'entrée du CONTEXT0 et on  
20 complémente la valeur de RND1. Dans l'exemple, on obtient RND1=0. On va alors exécuter l'autre séquence SEQA de T1, T2, T3 dans laquelle on utilise la première table de constante dans les trois tours T1, T2 et T3. On sauvegarde les paramètres de sortie (valeurs justes)  
25 dans une zone mémoire temporaire notée CONTEXT1.

Si FR est à 1, c'est que l'on a effectué les deux séquences. On restaure alors CONTEXT1 pour fournir les résultats intermédiaires L3, R3 ayant les valeurs justes, au tour suivant (T4).

30 Si RND1 vaut zéro, on commence par T1(TC<sub>0</sub>), T2(TC<sub>0</sub>), T3(TC<sub>0</sub>) et on finit par T1(TC<sub>1</sub>), T2(TC<sub>0</sub>), T3(TC<sub>0</sub>).

Arrivé à la fin du tour T13, on sauvegarde les paramètres fournis par ce tour, L13, R13, dans la  
35 mémoire temporaire CONTEXT0, et on procède pour les

tours restants T14, T15 et T16 de façon similaire aux premiers tours.

Dans tous les cas, il faut que le nombre d'instructions soit exactement le même quel que soit le chemin de calcul. C'est pour cela notamment que dans  
5 l'exemple d'application décrit, on prévoit de sauvegarder aussi les valeurs fausses (L3', R3' ou L16', R16') dans la zone mémoire temporaire CONTEXT2.

En effet si une différence quelconque existait  
10 entre les deux chemins possibles, il y aurait alors une possibilité d'attaque DPA fructueuse.

Le procédé de contre-mesure selon l'invention n'est pas limité à l'exemple particulier de réalisation décrit en référence à l'algorithme DES. Il s'applique à  
15 tout algorithme de cryptographie à clé secrète. De manière générale, pour toute mise en oeuvre d'un algorithme comprenant l'utilisation de premiers moyens pour fournir une donnée de sortie à partir d'une donnée d'entrée, la donnée de sortie et/ou des données  
20 dérivées étant manipulées par des instructions critiques, le procédé de contre-mesure selon l'invention comprend l'utilisation d'autres moyens, en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

25 L'utilisation des différents moyens, c'est à dire des premiers moyens et des autres moyens, est gérée selon une loi statistique de probabilité un demi.

Les autres moyens peuvent comprendre plusieurs moyens différents. Ils sont tels qu'à l'une ou à  
30 l'autre des données d'entrée et de sortie des premiers moyens, ils font correspondre la donnée complémentée.

Dans l'exemple d'un mode d'application du procédé de contre-mesure au DES plus particulièrement décrit, les premiers moyens consistent en la première table de  
35 constantes TC<sub>0</sub>. Les autres moyens consistent, en début de DES, dans la deuxième table de constantes TC<sub>1</sub>. En

fin de DES, ils consistent en deux tables de constantes différentes,  $TC_1$  et  $TC_2$  dans l'exemple.

Pour appliquer le procédé de contre-mesure selon l'invention à un algorithme de cryptographie à clé secrète donné, il faut donc d'abord déterminer toutes les données de cet algorithme qui peuvent être prédites et toutes les instructions critiques au sens de l'attaque DPA manipulant ces données ou des données dérivées. Il faut ensuite identifier dans l'algorithme des premiers moyens et des autres moyens au sens de l'invention, en sorte que toutes les données manipulées par les instructions critiques soient imprédictibles. Les premiers moyens sont, pour l'algorithme DES, la table de constantes  $TC_0$ . Les autres moyens sont dans l'exemple, d'autres tables de constantes. Ces moyens peuvent être des opérations différentes pour d'autres algorithmes. Pour un même algorithme, ces moyens peuvent consister en des opérations différentes selon les instructions critiques identifiées.

Le composant électronique 1 mettant en oeuvre un tel procédé de contre-mesure dans un algorithme de cryptographie à clé secrète comprend typiquement, comme représenté sur la figure 12, un microprocesseur  $\mu P$ , une mémoire programme 2 et une mémoire de travail 3. Pour pouvoir gérer l'utilisation des différents moyens selon l'invention, qui sont, dans l'exemple décrit, les différentes tables de constantes mémorisées en mémoire programme, des moyens 4 de génération d'une valeur aléatoire entre 0 et 1, sont prévus qui, si on se reporte à la figure 11, fourniront la valeur de RND1 à chaque exécution du DES. Un tel composant peut tout particulièrement être utilisé dans une carte à puce CP, pour améliorer leur inviolabilité.



## REVENDICATIONS

1. Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé secrète (K), la mise en oeuvre de l'algorithme comprenant l'utilisation de premiers  
5 moyens ( $TC_0$ ) pour fournir une donnée de sortie (S) à partir d'une donnée d'entrée (E), la donnée de sortie et/ou des données dérivées étant manipulées par des instructions critiques, caractérisé en ce que le procédé de contre-mesure prévoit l'utilisation d'autres  
10 moyens ( $TC_1$ ), en sorte que la donnée de sortie et les données dérivées soient imprédictibles.

2. Procédé de contre-mesure selon la revendication 1, caractérisé en ce que l'utilisation des différents  
15 moyens ( $TC_0$ ,  $TC_1$ ) est gérée par une loi statistique de probabilité un demi.

3. Procédé de contre-mesure selon la revendication 2, la mise en oeuvre de l'algorithme comprenant seize  
20 tours de calcul ( $T_1$ , ...,  $T_{16}$ ), caractérisé en ce qu'il comprend l'exécution d'une première séquence (SEQA) et d'une deuxième séquence (SEQB) formées des trois premiers tours au moins ( $T_1$ ,  $T_2$ ,  $T_3$ ), l'ordre d'exécution des séquences étant fonction de la loi  
25 statistique de probabilité un demi, la première séquence (SEQA) utilisant les premiers moyens ( $TC_0$ ) dans chaque tour, la deuxième séquence (SEQB) utilisant les autres moyens ( $TC_1$ ) dans le premier tour ( $T_1$ ) au moins.

30

4. Procédé de contre-mesure selon la revendication 3, caractérisé en ce que la première et la deuxième

séquences sont formées chacune des trois premiers tours (T1, T2, T3).

5        3 ou 4, caractérisé en ce que les autres moyens  
consistent en des deuxièmes moyens ( $TC_1$ ) tels que pour  
une même donnée d'entrée (E), ils fournissent en sortie  
le complément (/S) de la donnée de sortie (S) des  
premiers moyens ( $TC_0$ ).

10

6. Procédé de contre-mesure selon la revendication  
2, la mise en oeuvre de l'algorithme comprenant seize  
tours de calcul (T1, ..., T16), caractérisé en ce qu'il  
comprend l'exécution d'une première séquence (SEQA') et  
15 d'une deuxième séquence (SEQB') formées chacune des  
trois derniers tours (T14, T15, T16) au moins, l'ordre  
d'exécution des séquences étant fonction de la loi  
statistique de probabilité un demi, la première  
séquence (SEQA') utilisant les premiers moyens ( $TC_0$ )  
20 dans chaque tour, la deuxième séquence (SEQB')  
utilisant les autres moyens ( $TC_1$ ,  $TC_2$ ).

7. Procédé de contre-mesure selon la revendication  
6, caractérisé en ce que la première et la deuxième  
séquences sont formées chacune des trois derniers  
25 tours, et en ce que les autres moyens utilisés dans la  
deuxième séquence comprennent des deuxièmes moyens  
( $TC_1$ ) et des troisièmes moyens ( $TC_2$ ).

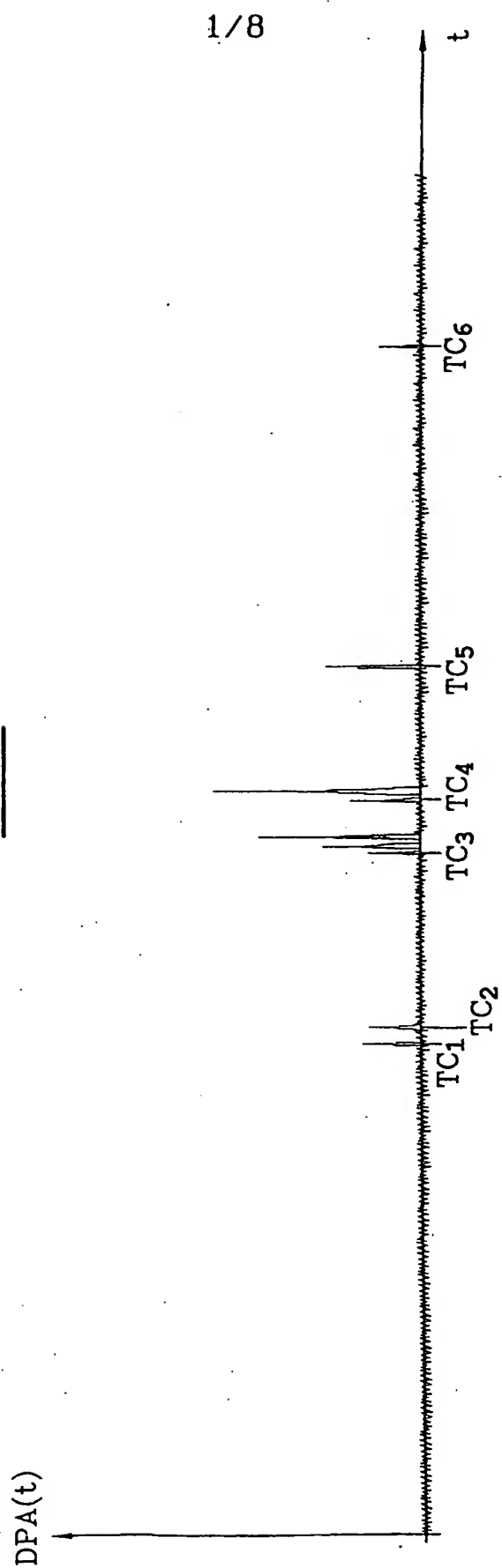
30        8. Procédé de contre-mesure selon la revendication  
6 ou 7, caractérisé en ce que les deuxièmes moyens  
( $TC_1$ ) sont tels que pour une même donnée d'entrée (E),  
ils fournissent en sortie le complément (/S) de la  
donnée de sortie (S) des premiers moyens ( $TC_0$ ) et en ce  
35 que ces deuxièmes moyens sont utilisés dans la deuxième  
séquence (SEQB') pour le quatorzième tour (T14).

9. Procédé de contre-mesure selon la revendication 8, caractérisé en ce que les troisièmes moyens ( $TC_2$ ) sont tels que pour le complément de la donnée d'entrée (E), ils fournissent en sortie le complément (/S) de la donnée de sortie (S) des premiers moyens ( $TC_0$ ) et sont utilisés dans la deuxième séquence, pour le quinzième tour et le seizième tour (T15, T16).

10. Procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens sont des tables de constantes.

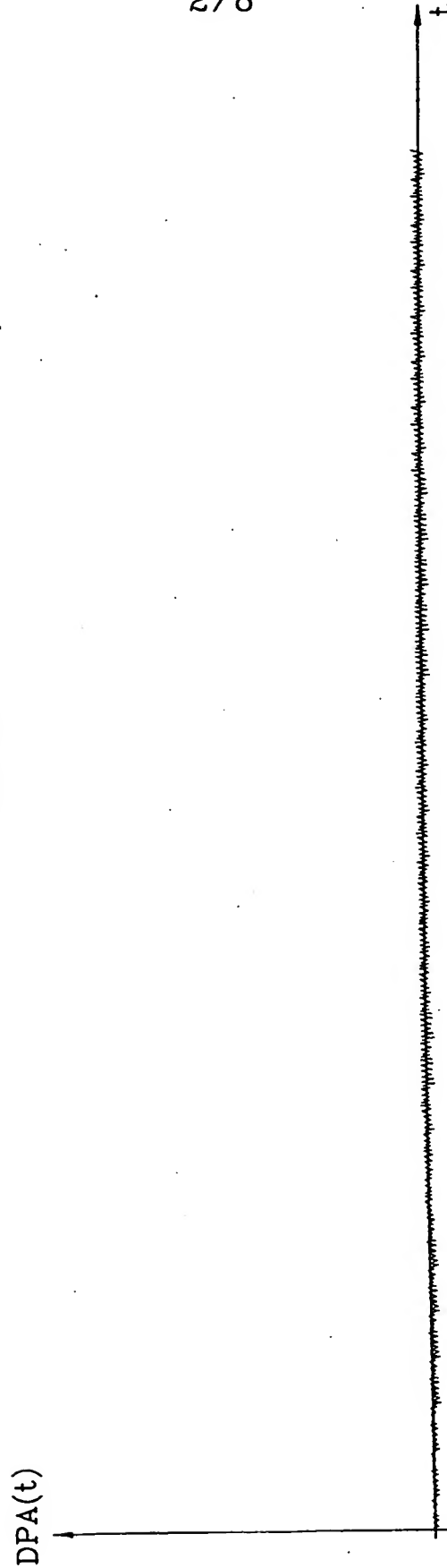
11. Composant électronique mettant en oeuvre le procédé de contre-mesure selon l'une quelconque des revendications précédentes, caractérisé en ce que les différents moyens ( $TC_0$ ,  $TC_1$ ,  $TC_2$ ) pour fournir une donnée de sortie à partir d'une donnée d'entrée sont fixés en mémoire programme du dit composant et en ce qu'il comprend des moyens de génération d'une valeur aléatoire (RND1) à 0 ou à 1 pour gérer l'utilisation des dits différents moyens.

12. Carte à puce comprenant un composant électronique selon la revendication 11.

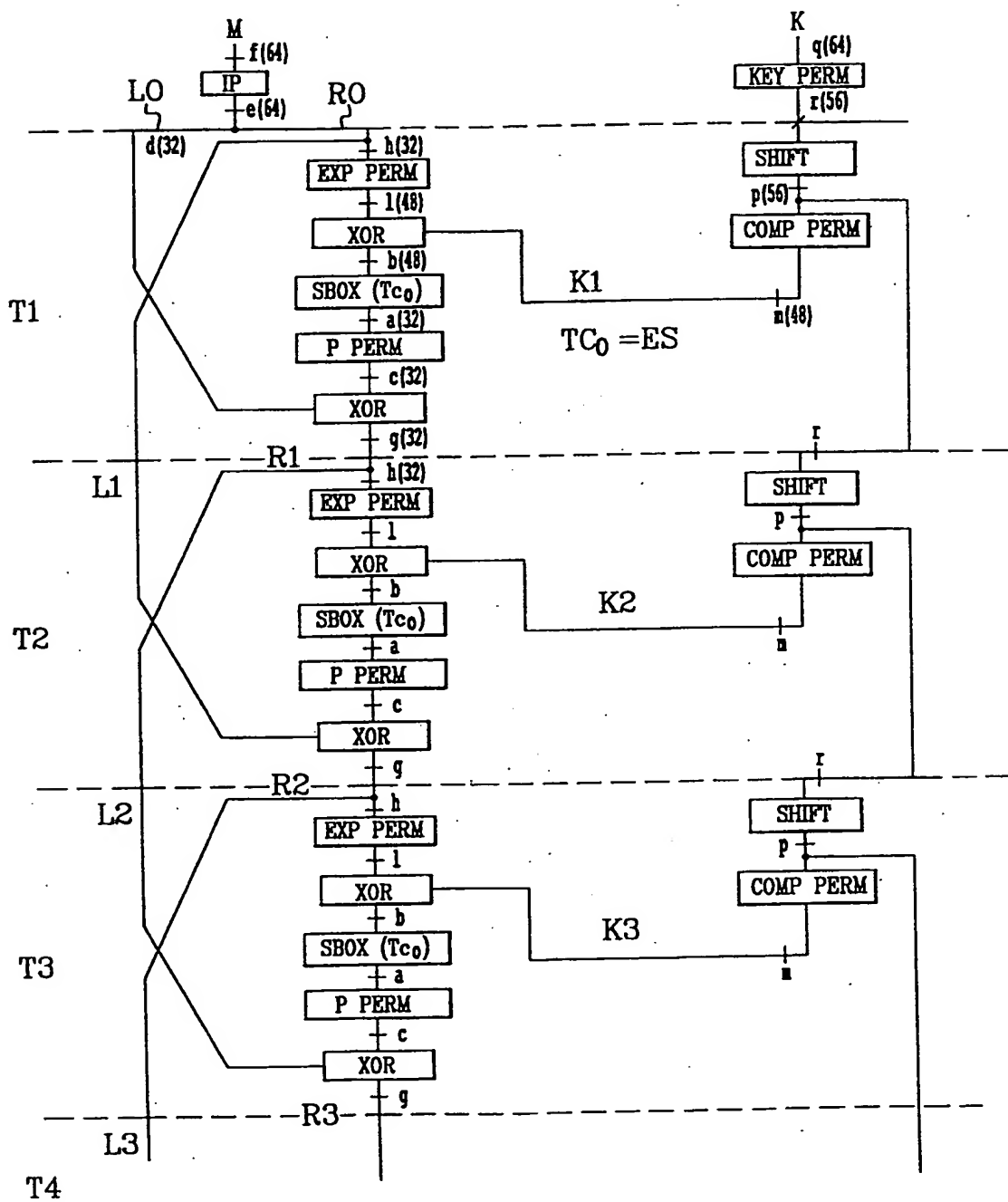
**FIG.1**

2/8

FIG. 2



3/8

**FIG.3**

4/8

T13

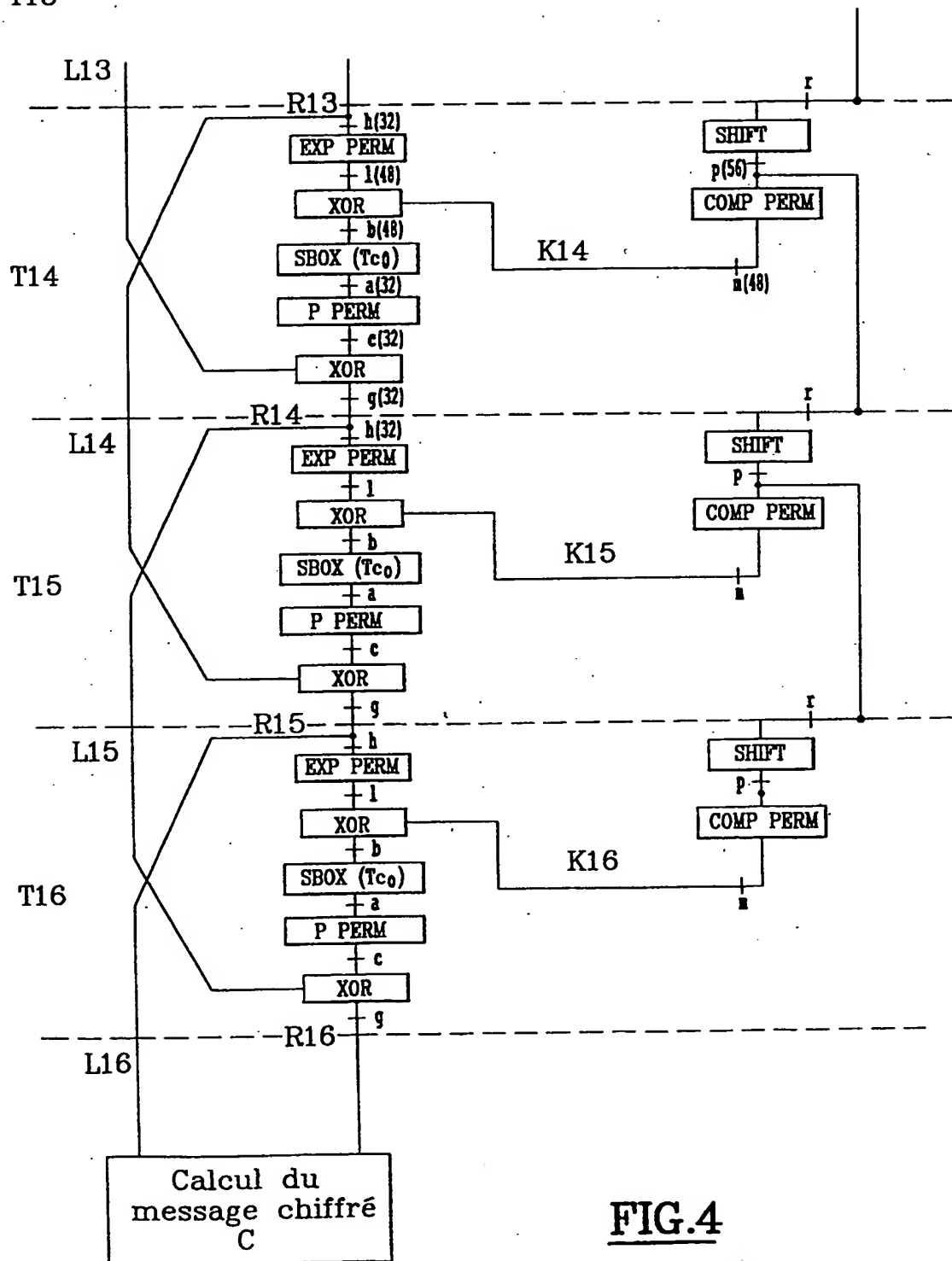
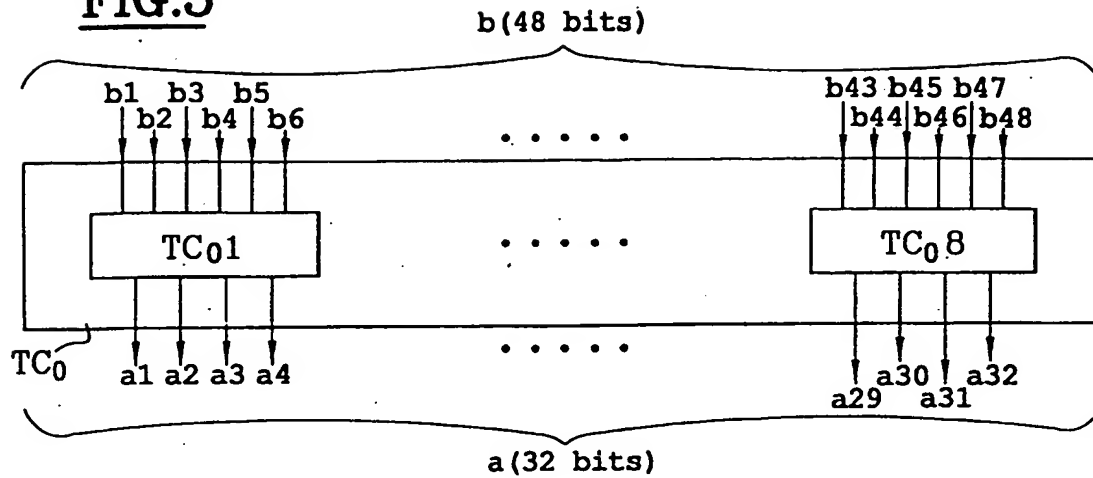


FIG.4

5/8

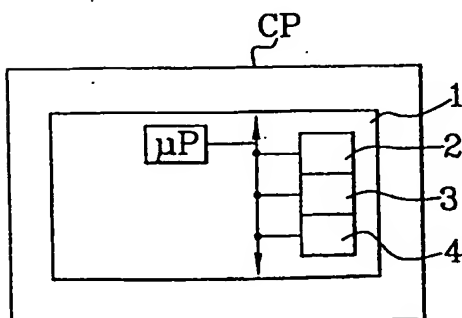
**FIG.5****FIG.6**

$TC_0 1$	$E1=b1b2b3b4b5b6$	$S1=a1a2a3a4$
	000000	1101
	000001	0101
	$\vdots$	$\vdots$
	111111	1010

$E1=b1b2b3b4b5b6$	$/S1=a1a2a3a4$	$TC_1 1$
000000	0010	
000001	1010	
$\vdots$	$\vdots$	
111111	0101	

**FIG.9**

$TC_2 1$	$/E1=b1b2b3b4b5b6$	$/S1=a1a2a3a4$
	000000	0101
	$\vdots$	$\vdots$
	111110	1010
	111111	0010

**FIG.10****FIG.12**



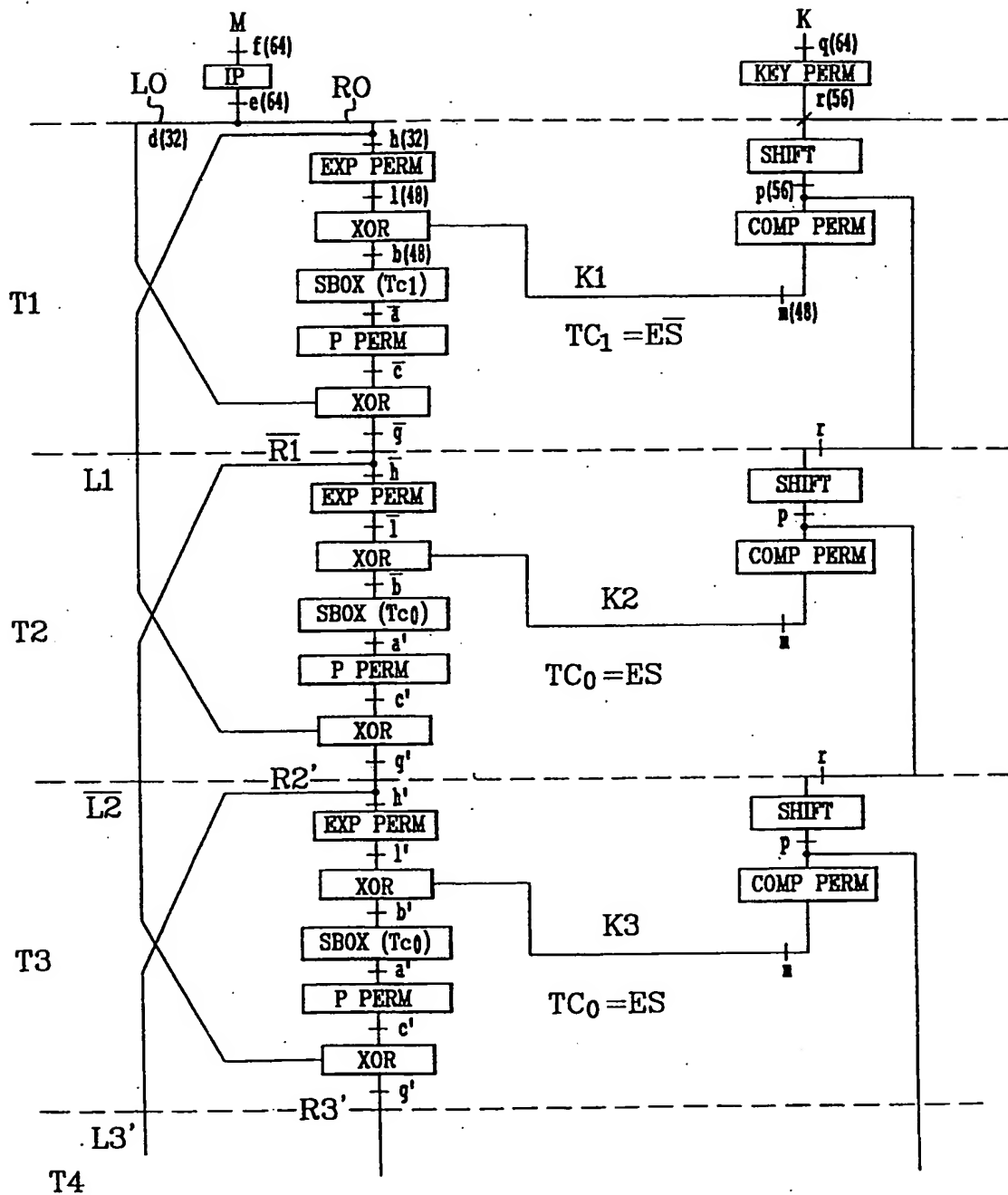
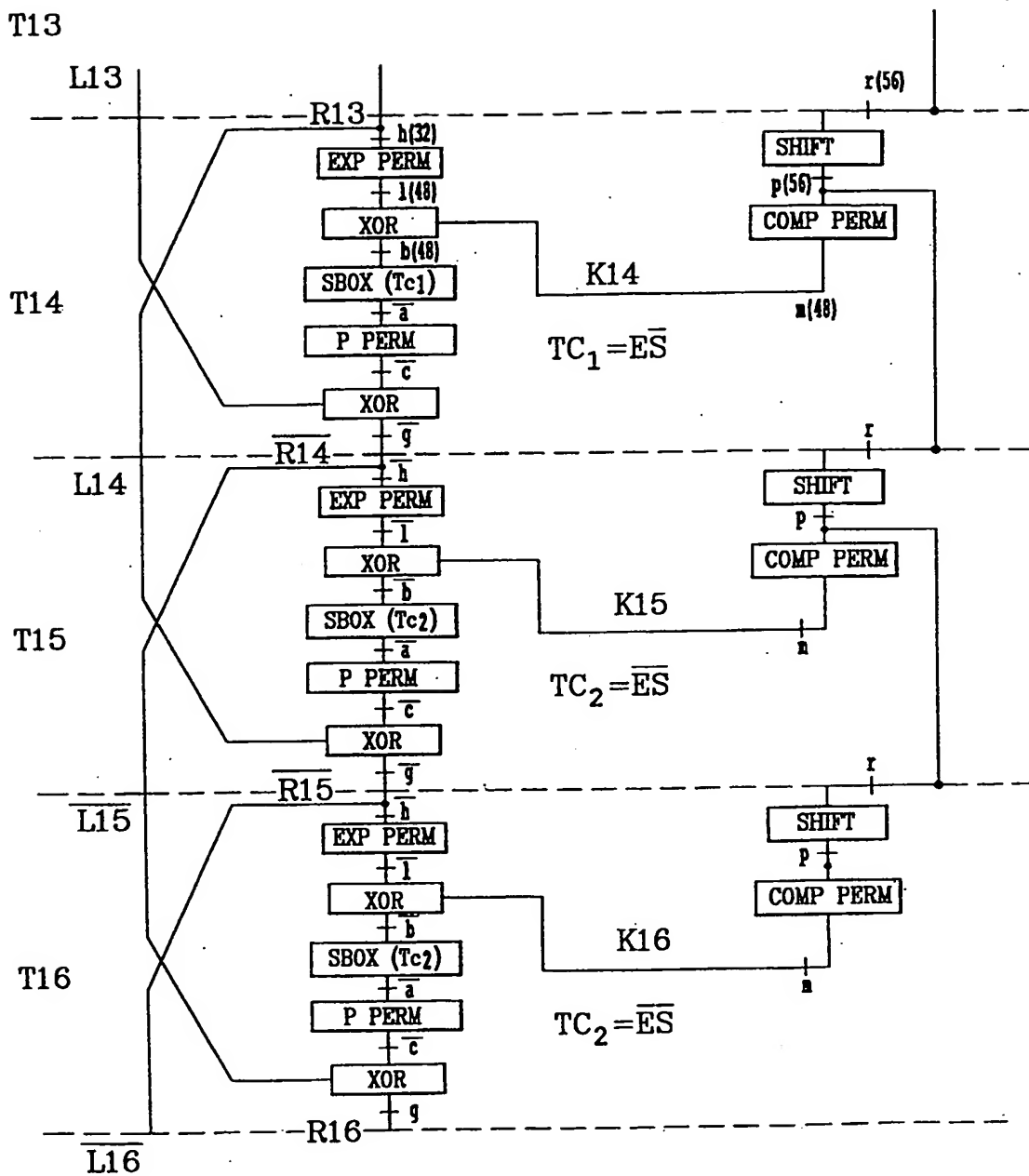


FIG.7



**FIG.8**

8/8

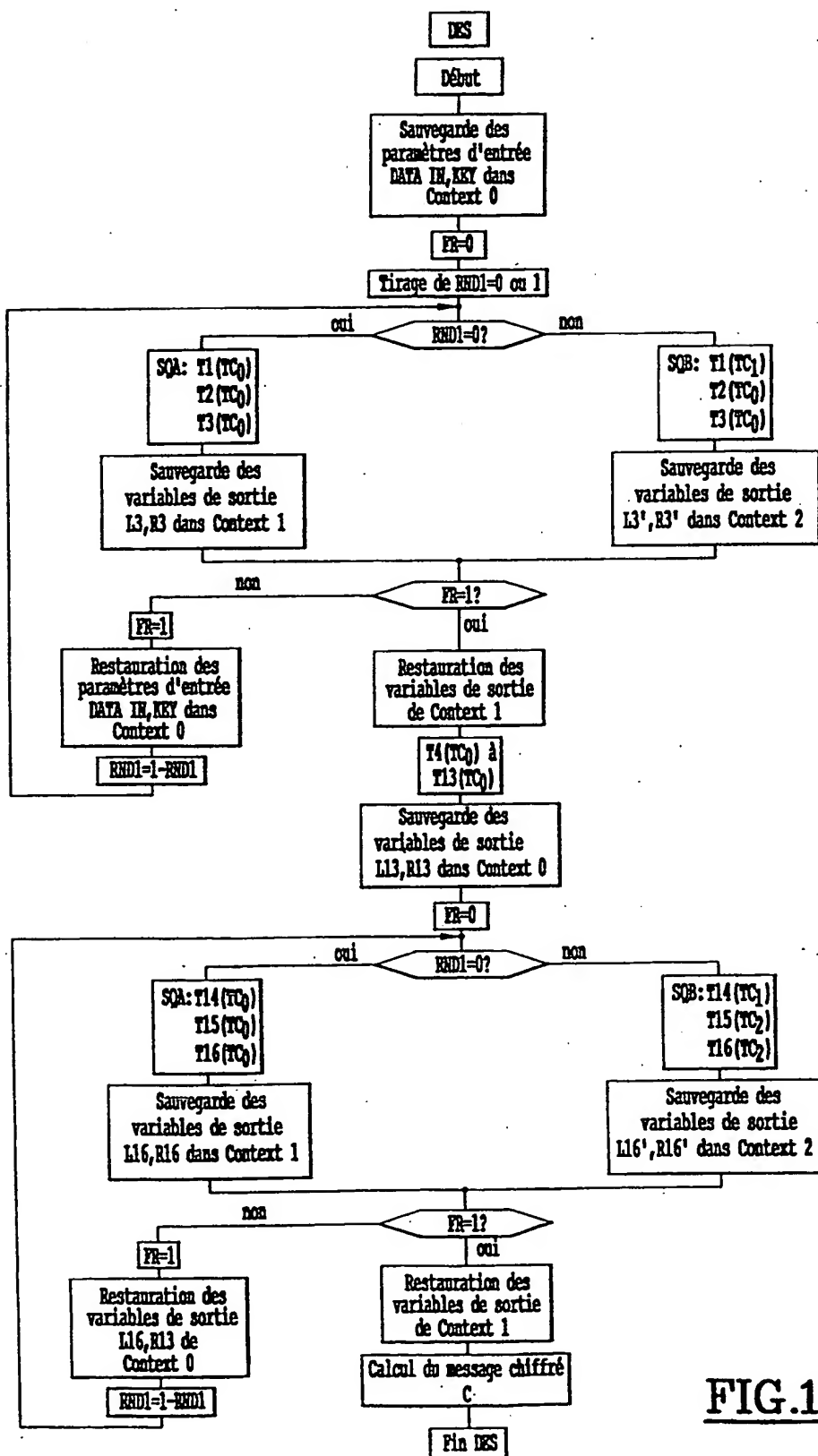


FIG.11

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR 99/02172

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 November 1997 (1997-11-03), pages 689-693, XP000737626</p> <p>INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS</p> <p>abstract</p> <p>column 1, line 13 - line 29</p> <p>column 2, line 6 - line 18</p> <p>column 3, line 1 - column 5, line 1</p> <p style="text-align: center;">-/-</p>	1,2,10



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

**\* Special categories of cited documents:**

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

10 January 2000

Date of mailing of the international search report

18/01/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Gautier, L

# INTERNATIONAL SEARCH REPORT

International Application No.

PCT/FR 99/02172

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 July 1994 (1994-07-01), pages 85-90, XP000460342 the whole document	1
A	FR 2 672 402 A (GEMPLUS CARD INT) 7 August 1992 (1992-08-07) abstract page 1, line 4 - line 12 page 3, line 19 - line 23 figure 1 claim 1	11,12

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 99/02172

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2672402 A	07-08-1992	NONE	

# RAPPORT DE RECHERCHE INTERNATIONALE

Dem. internationale No

PCT/FR 99/02172

A. CLASSEMENT DE L'OBJET DE LA DEMANDE  
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>YI X ET AL: "A METHOD FOR OBTAINING CRYPTOGRAPHICALLY STRONG 8X8 S-BOXES" IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, PHOENIX, ARIZONA, NOV. 3 - 8, 1997, vol. 2, 3 novembre 1997 (1997-11-03), pages 689-693, XP000737626</p> <p>INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS</p> <p>abrégé</p> <p>colonne 1, ligne 13 - ligne 29</p> <p>colonne 2, ligne 6 - ligne 18</p> <p>colonne 3, ligne 1 -colonne 5, ligne 1</p> <p style="text-align: center;">-/-</p>	1,2,10

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent: l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent: l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

10 janvier 2000

Date d'expédition du présent rapport de recherche internationale

18/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3018

Fonctionnaire autorisé

Gautier, L

# RAPPORT DE RECHERCHE INTERNATIONALE

Dema. internationale No  
PCT/FR 99/02172

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MIYAGUCHI S: "SECRET KEY CIPHERS THAT CHANGE THE ENCIPHERMENT ALGORITHM UNDER THE CONTROL OF THE KEY" NTT REVIEW, vol. 6, no. 4, 1 juillet 1994 (1994-07-01), pages 85-90, XP000460342 le document en entier	1
A	FR 2 672 402 A (GEMPLUS CARD INT) 7 août 1992 (1992-08-07) abrégé page 1, ligne 4 - ligne 12 page 3, ligne 19 - ligne 23 figure 1 revendication 1	11,12



# RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No

PCT/FR 99/02172

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2672402 A	07-08-1992	AUCUN	